Shantanu Rane

Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94304
srane@parc.com, 650-812-4409
https://shantanudrane.github.io

About

I lead a research group dedicated to the design, modeling, security and privacy of cyber-physical systems. My expertise is in the areas of applied cryptography, signal processing and machine learning.

Professional Experience

2014 –	**Palo Alto Research Center (PARC)**
2017 –	Research Area Manager
2014 – 17	Senior Member Research Staff
2007 – 14	**Mitsubishi Electric Research Labs (MERL)**
2010 – 14	Principal Research Scientist
2007 – 10	Research Scientist

Education

2007	Ph.D., Electrical Engineering Stanford University, GPA 3.72
2001	M.S., Electrical Engineering University of Minnesota, GPA 3.93
1999	B. E., Instrumentation Engineering University of Pune, India, Rank 1/360

Publication Record

# papers	79
# patents	58
# cites	> 5678 (as of March 2022)
h-index	33
i10-index	64

Grants

2017 – 22	$3,500,000, DARPA Configuration Security Project: Secure Configurations for the IoT Based on Optimization and Reasoning on Graphs. **(Co-PI)**
2019 – 21	$1,000,000, DARPA Quantifying Ensemble Diversity for Robust Machine Learning (QED for RML), Project: Ikebana: Robust Arrangements of Classifiers in Version Space. **(PI)**
2020 – 21	$454,000, DARPA Techniques for Machine Vision Disruption (TMVD), Collaboration with University of California at Riverside. **(Subcontract PI)**
2017 – 19	$200,000, DHS, Project in collaboration with Rutgers University: Differentially Private Anomaly Detection (DPAD) Phase II and III. **(Subcontract PI)**

Key Projects

2019 – PARC	**Machine Learning Security:** Research on understanding the role of adversarial examples against neural networks, and crafting defenses against them. 2019 PARC Excellence Award.
2018 – PARC	**Distributed System Security:** Developing approaches to optimize the security and functionality of IoT systems, using multilayer graphs and Satisfiability Modulo Theory (SMT) solvers.
2017 – 19 PARC	**Differential Privacy:** Research on privacy-aware training of active machine learning algorithms, with tradeoffs among privacy, accuracy, speed, scalability.
2014 – 16 PARC	**Privacy-preserving analytics:** Use of homomorphic encryption and secure multiparty computation for aggregate analytics on encrypted data. 2015 PARC Exceptional Achievement Award.
2009 – 14 MERL	**Secure computation:** Research on using approaches from signal processing and cryptography for nearest neighbor

computations over sensitive data. 2010 MERL Directors Award.

2008 – 14 MERL — **Secure Biometrics:** Fundamental and applied research on biometric template protection. US National Body delegate in the ISO/IEC JTC1 SC37 Biometrics Subcommittee. Editor of working draft of international standard for evaluation of template protection schemes.

2009 – 12 MERL — **SAR Compression:** Developed a SAR raw data compression scheme for a successful Mitsubishi Electric contract for onboard compression module of Advanced Land Observations Satellite (ALOS-2), launched by JAXA in 2014.

2001 – 07 Stanford — **Error-resilient video transmission:** Thesis on Systematic Lossy Error Protection (SLEP) based on distributed source coding. With theoretical analysis, modeling, H.264/AVC implementation.

Key Professional Activities

2018 – 20, 2012 – 15 — Associate Editor, IEEE Transactions on Information Forensics and Security.

2012 – 14 — Associate Editor, IEEE Signal Processing Letters.

2014 — Technical Co-Chair, IEEE Workshop in Information Forensics and Security.

2011 – 13 — Elected to IEEE Information Forensics and Security Technical Committee.

Selected Publications

2005 — B. Girod, A. Aaron, S. Rane, and D. Rebollo-Monedero, Distributed Video Coding, Proceedings of the IEEE.

2010 — M. Pathak, S. Rane, and B. Raj, Multiparty Differential Privacy via Aggregation of Locally Trained Classifiers, Neural Information Processing Conference.

2013 — S. Rane and P. Boufounos, Privacy-Preserving Nearest Neighbors, IEEE Signal Processing Magazine.

2017 — P. Boufounos, S. Rane and H. Mansour, Representation and Coding of Signal Geometry, Information and Inference.

2020 — H. Soroush, M. Albanese, M. A. Mehrabadi, I. Iganibo, M. Mosko, J. Gao, D. Fritz, S. Rane and E. Bier, SCIBORG: Secure Configurations for the IoT Based on Optimization and Reasoning on Graphs, IEEE Conference on Networking and Security. Best Paper Award.

2020 — D. Bittner, A. Brito, M. Ghassemi, S. Rane, A. Sarwate and R. Wright, Understanding Privacy-Utility Tradeoffs in Differentially Private Online Active Learning, Journal of Privacy and Confidentiality.

2021 — Z. Cai, S. Rane, A. Brito, C. Song, S. Krishnamurthy, A. Roy-Chowdhury, Zero Query Transfer Attacks on Context Aware Detectors, IEEE Computer Vision and Pattern Recognition (CVPR).

Selected Talks

2018 — **Keynote:** A Cyber-Physical Systems Perspective on Biometric Security and Privacy, IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Los Angeles, CA.

2015 — **Tutorial:** Privacy-Aware Data Analytics, IEEE International Workshop on Information Forensics and Security, Rome, Italy.

2015 — **Keynote:** Building Privacy-Aware Computing Systems, High Confidence Software Systems, Annapolis, MD.

2013 — **Tutorial:** Secure Biometrics: Concepts, Architectures and Challenges, IAPR International Conference on Biometrics, Madrid, Spain.